Claims

What is claimed is:

1. A computer system and one or more trusted modules associated with the computer system where the computer system can generate cryptographic tickets intended to be transmitted to one or more of the trusted modules allowing intended trusted modules to issue a set quantity of public-key certificates on request from users of the trusted modules, the certificates issued by the trusted modules consisting of (i) components that are constrained by the trusted module and (ii) other components of the certificates able to be specified by the requesting user.
2. A computer system based on claim 1 where the trusted module is a tamper-proof hardware security module or a USB token or a smartcard.
3. A computer system based on claim 1 where the cryptographic ticket is a public-key or private-key certificate.
4. A computer system based on claim 3 where the trusted module is a tamper-proof hardware security module or a USB token or a smartcard.
5. A computer system based on claim 1 where the set quantity of certificates that can be issued is determined by information within the provided cryptographic ticket.
6. A computer system based on claim 5 where the trusted module is a tamper-proof hardware security module or a USB token or a smartcard.